



NOVA SCHOOL OF
BUSINESS & ECONOMICS

Operational Risk

1. What is the nature of the problem faced by Banc One in November 1993?
2. How does Banc One measure its interest rate risk exposure?
3. What sort of interest rate risk management is followed by Banc One? What is the rationale of the interest rate risk policy (asset sensitive) followed by this bank?
4. Why is Banc One using derivatives as part of its interest rate risk management? Could the same results be achieved without the use of derivatives? How? Which alternative is best for the bank?
5. Explain the logic behind the AIRS. Why is Banc One using them?
6. Explain the logic behind the basis swaps used by Banc One. Why is their total notional amount growing?
7. What are the risks associated with the use of derivatives in this context?
8. Are swaps distorting Banc One's reported earnings and risk?
9. Is the Bank's use of derivatives creating or destroying value? Why? What should the bank do?

Group 14

What is behind the Treasury sell-off?

The double whammy of falling bond and equity prices could partly be hedge funds unwinding so-called 'basis trades'

GILLIAN TETT

+ Add to myFT



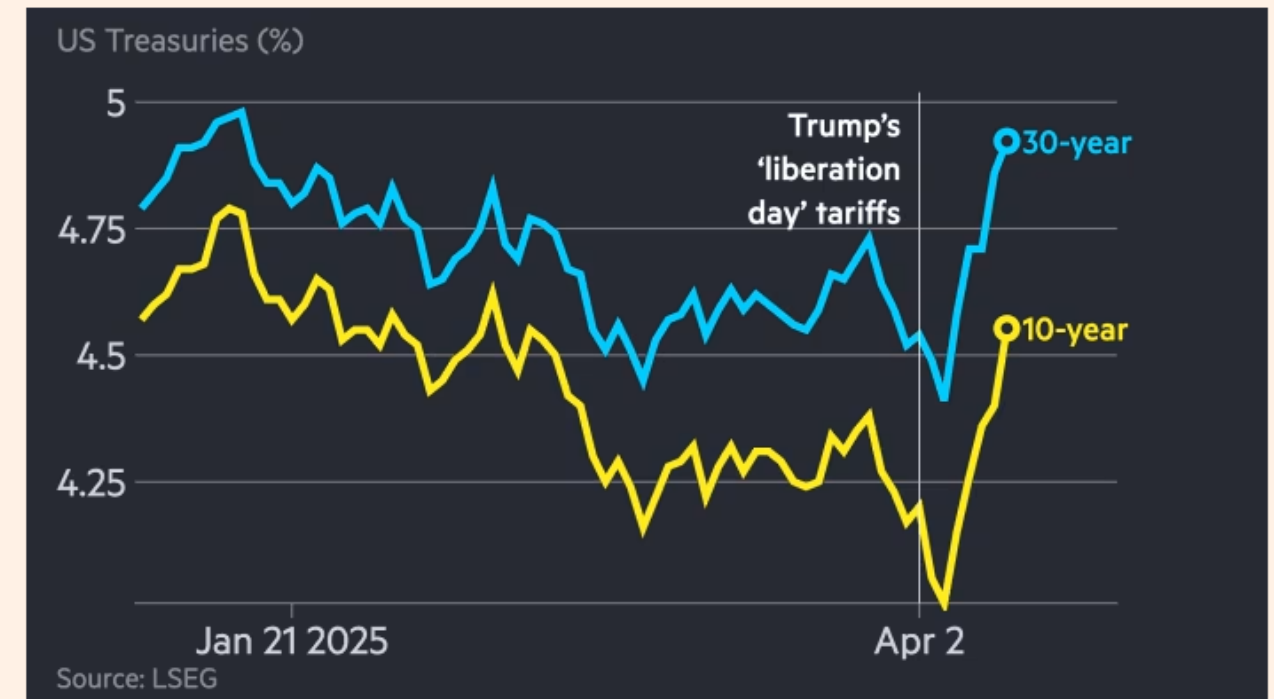
President Donald Trump holds up a signed executive order at the White House this week. Traders know that as a businessman, he repeatedly defaulted on his own debt © Alex Brandon/AP

Gillian Tett

Published APR 9 2025

Liquidity worsens in \$29tn Treasury market as volatility soars

10-year US government bond yield rose most this week since 2001



The 10-year Treasury yield climbed as much as 0.19 percentage points to 4.58 per cent

Kate Duguid and Harriet Clarfelt in New York and Costas Mourselas in London

Published APR 11 2025 | Updated APR 12 2025, 01:22

477

MENTI TIME 😊

Credit

Interest Rate

Market

Liquidity

Foreign Exchange

Off-Balance

Operational

Sovereign

Insolvency

- Operational risk deals with potential losses arising from failures due to systems, people (incompetence, negligence or fraud), suppliers, procedures, reputation.
- Every single day you can expect operational failures in a bank.
- Management of this type of risk depends on frequency and severity.

Risks arise also because of the **WAY** things are done and not only because of the assets & liabilities held by the bank at each moment.

Operational Risk

The trade-off

**CONTRADICTIONARY
PRINCIPLES**

It is impossible to
cover all risks

BUT

it is necessary to limit
risk-taking

Banks need to keep some
margin for business
growth

BUT

Banks need to invest in
suitable monitoring
systems

Banks need to
reduce
operating costs

BUT

Banks must implement
means to manage risks and
to develop appropriate
models

Operational Risk started to be addressed at the technology level:

- ✓ banks are large investors in IT systems;
- ✓ an error might have incredible costs (what about a miscalculated price on a large trade?);
- ✓ M&A in banking forced a lot of system integration, leaving systems more fragile;
- ✓ banks are suitable targets for hackers, as there is electronic money and most clients will not notice an undue transaction in time.

Operational Risk

IT: when it goes wrong

TSB swings into red in first half following IT debacle

Lender sets aside an extra £176m to deal with the aftermath of a disastrous upgrade



The costs of the IT crisis pushed TSB to its first ever loss © PA

Nicholas Megaw in London JULY 27, 2018



TSB's [IT fiasco](#) has so far cost it £176m, the UK bank said on Friday, with further charges expected to accumulate after customers were left unable to access their bank accounts.

The costs of the crisis lender avoided the

Banks under fire from parliament after IT outages at TSB and Ulster Bank

TSB chief 'truly sorry' and Ulster Bank suffers problems

Nicholas Megaw, Retail Banking Correspondent APRIL 24, 2018



The chair of the influential Treasury select committee Nicky Morgan railed against the "litany of failures of banking IT systems" on Tuesday, as customers at two different banks were left unable to access their funds.

TSB chief executive Paul Pester said he was "truly sorry" for a [botched IT switchover](#) that has prompted inquiries from both the UK's privacy watchdog and Financial Conduct Authority.

Meanwhile Ulster Bank, the Irish arm of [Royal Bank of Scotland](#), said it had launched an urgent investigation after complaints that transactions that had previously been made to accounts since last Friday were no longer showing for many customers, leaving some overdrawn and unable to make payments.

Best of Money: hacking into your account is easier than you think

Fake fingerprints, selfie masks and voice tapping mean the wealthy should be worried



© James Minchall

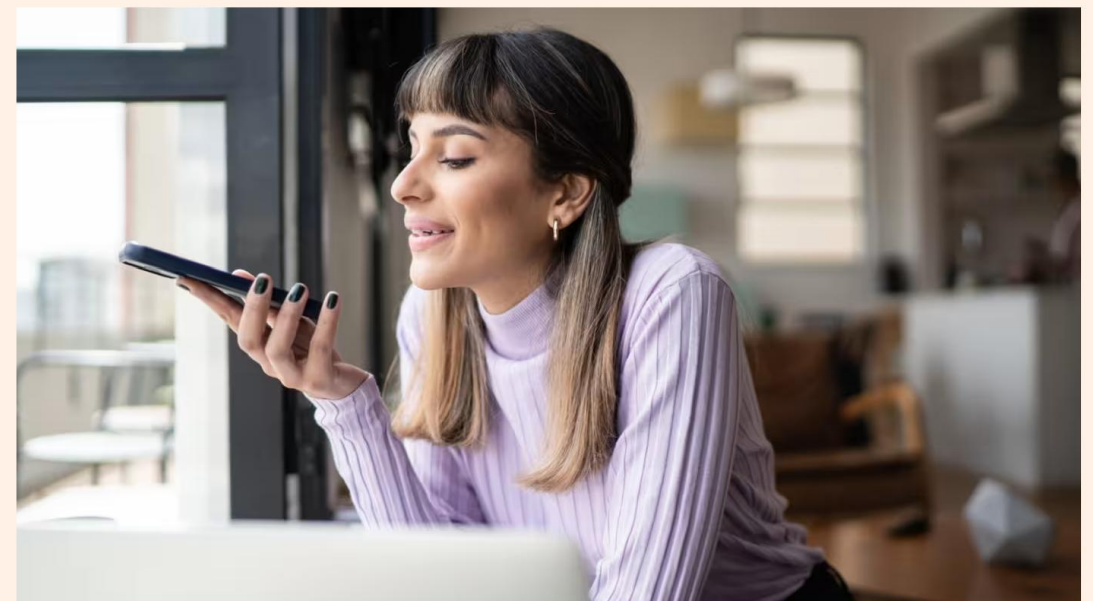
Martin Arnold and Hugo Greenhalgh NOVEMBER 4, 2016



Anyone who has ever struggled to reapp or fumbled with a card-reading or their fingerprint, voice or face to access a smartphone.

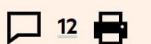
UK banks prepare for deepfake fraud wave

Experts warn that rapidly developing technology threatens to 'put financial crime on steroids'



Deepfakes and voice cloning are getting easier to generate, meaning scammers have the potential to target far more people and with a higher rate of success © Getty Images

Akila Quinio in London JANUARY 19 2024



MENTI TIME 😊

Operational Risk

Murphy's Law?

People	Systems	Processes	External Events
Fraud, collusion and other criminal activities	IT problems (hardware, software, hacking, viruses)	Execution, registration, settlement and documentation errors	Criminal activities (theft, vandalism, terrorism)
Violation of internal or external rules (secrecy, ethical rules, the law)	Software bugs	Errors in models, methodologies and mark to market	Political and military events (war, coup d'état, international sanctions)
Incompetence or negligence	Unauthorized access to information	Compliance errors (accounting, taxation, reporting)	Changes in the political, legal, regulatory and tax environment
Loss of important employees (illness, problems retaining staff)	Unavailable and questionable integrity of data	Inadequate procedures, bad business practices	Natural events (fire, flood, earthquakes)
Violations of system securities	Utility outages (power, telecoms)	Inadequate definition and attribution of responsibilities	Operational failure at suppliers and outsourcers

This table is taken, with adaptation, from Resti and Sironi.

Operational Risk

A special kind?

Financial Risks	Operational Risk
Consciously and willingly faced	Unavoidable
Speculative risks, implying profits or losses	Pure risks, implying losses only
Consistent with an increasing relationship between risk and expected return	Not consistent with an increasing relationship between risk and expected return
Easy to identify and understand	Difficult to identify and understand
Comparatively easy to measure and quantify	Difficult to measure and quantify
Large availability of hedging instruments	Lack of effective hedging instruments
Comparatively easy to price and transfer	Difficult to price and transfer

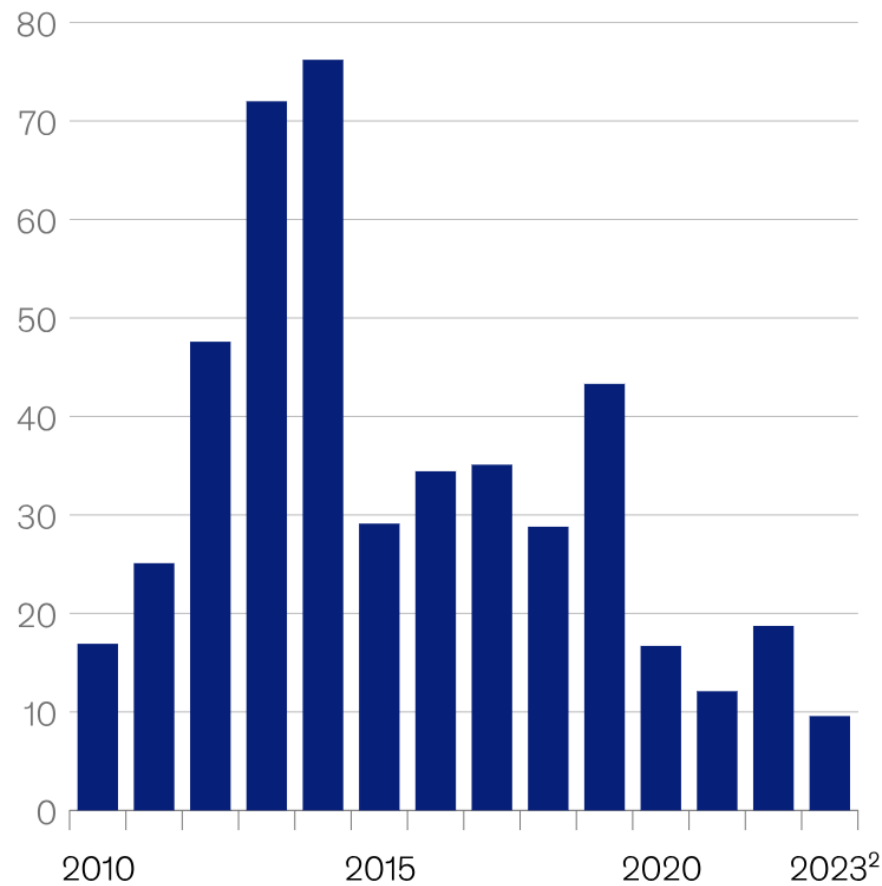
Source: Resti and Sironi.

Operational Risk

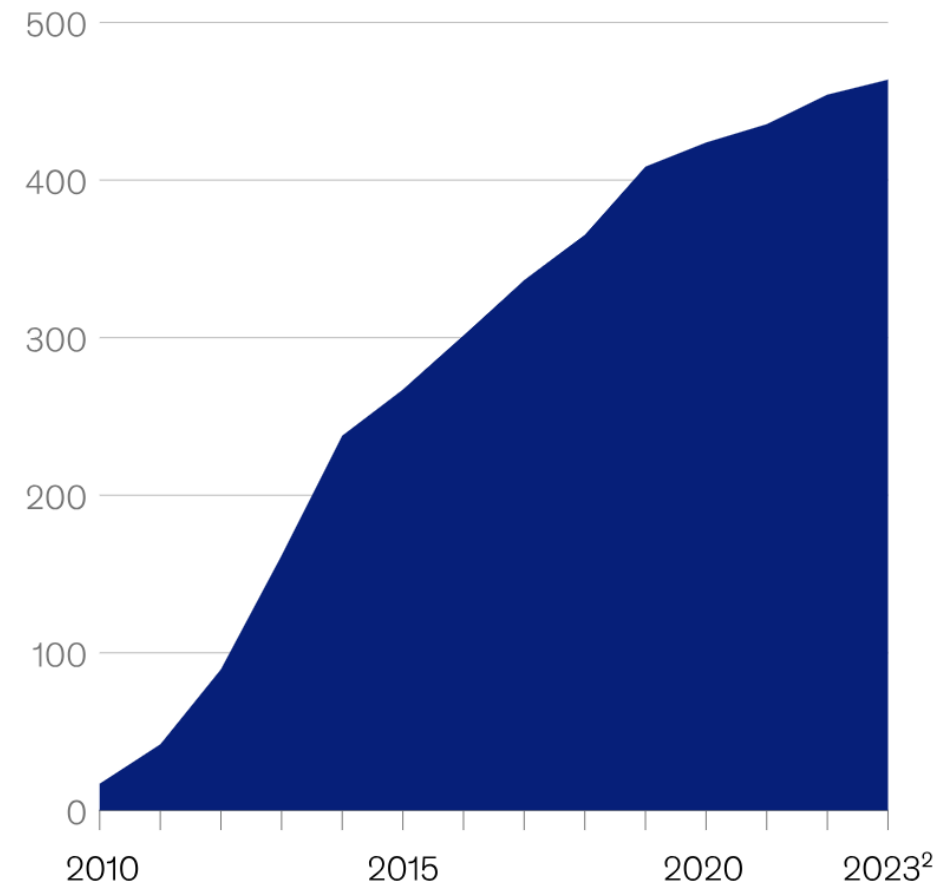
It's no free lunch

Operational losses, fines, and litigation costs for nonfinancial risks have cumulated to approximately \$460 billion over the past 14 years.

Operational losses, fines, and litigation costs 2010–23,¹ \$ billion (annually)



Operational losses, fines, and litigation costs 2010–23, \$ billion (cumulative)



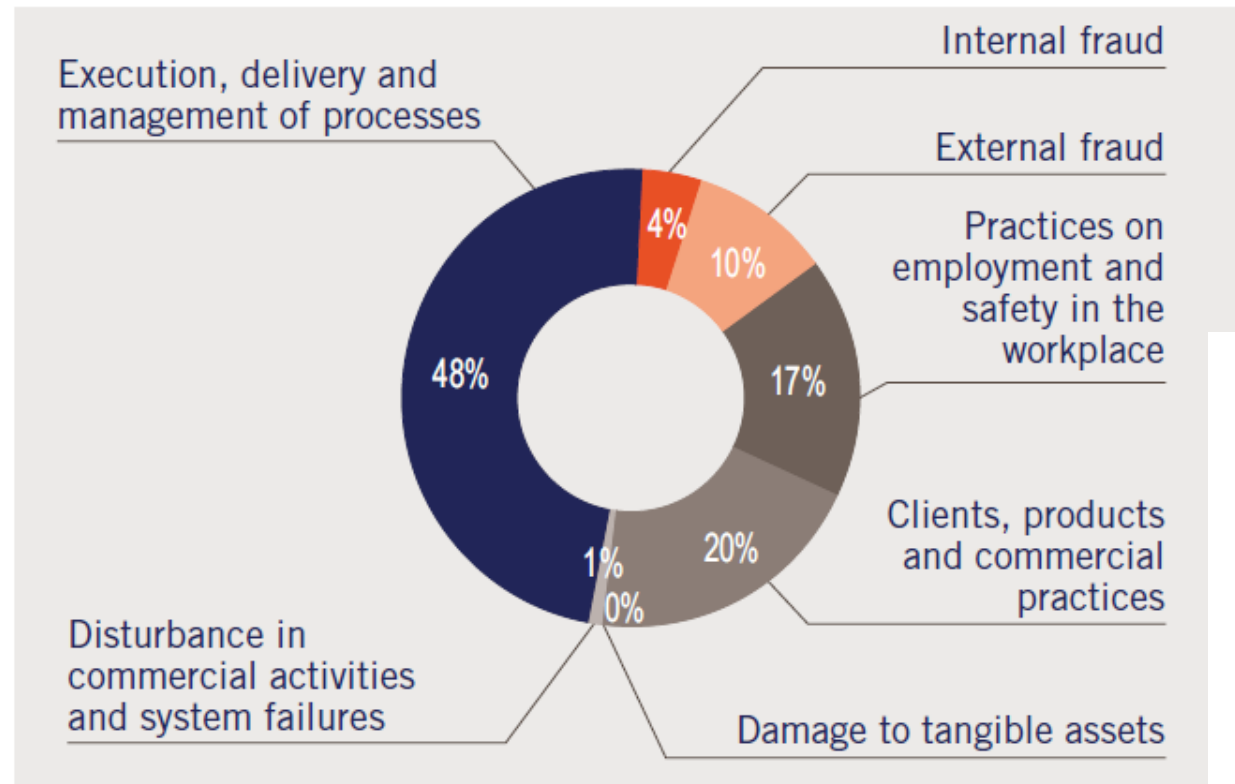
¹Includes operational risk losses (eg, unauthorized trading), fines, settlements, and expenses for provision buildup (eg, provisions for compensating customers). Based on incidents settled/expensed and gathered through news and press search. Sample of European and US banks totals 304, comprising 830 event/fine/cost entries.

²Year-to-date Jan–Aug 2023.

Operational Risk

Main categories

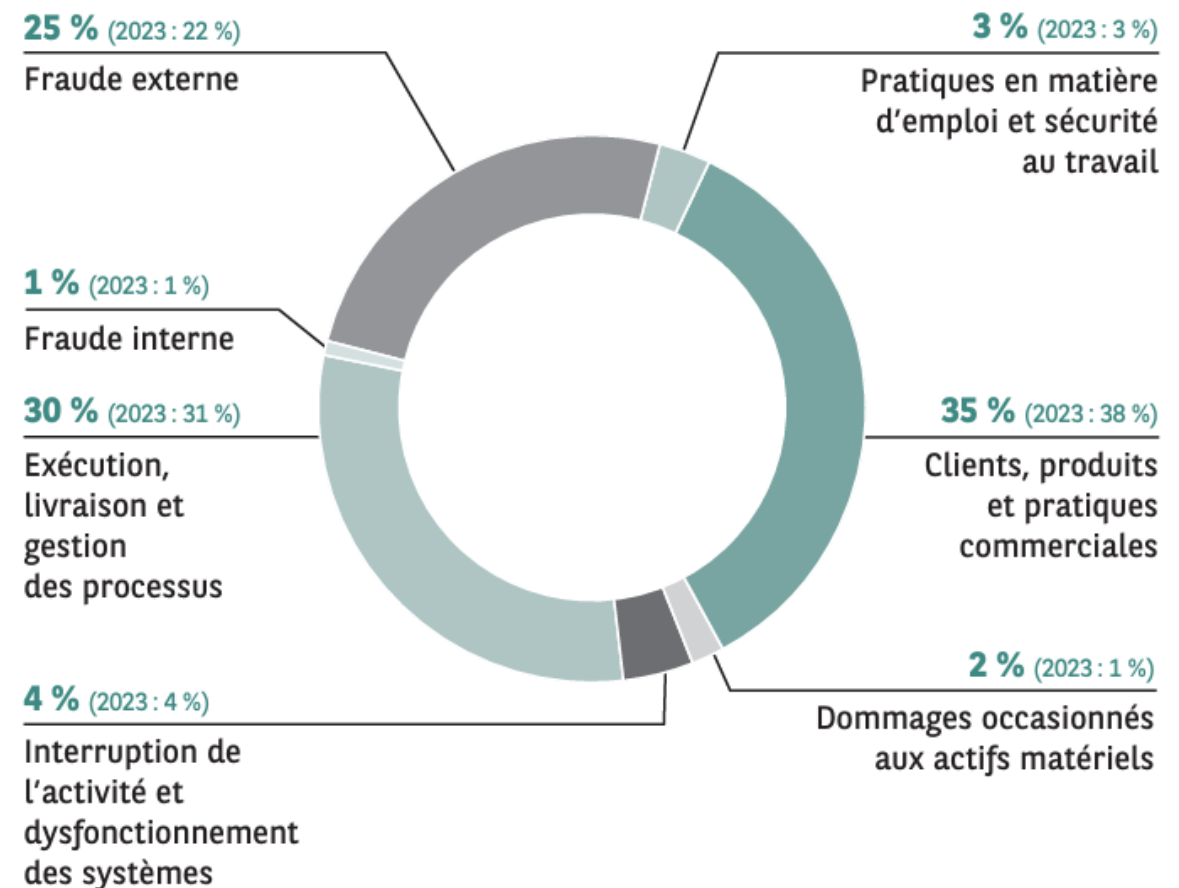
Breakdown of gross losses by type of risk
In 2018



Source: BPI 2018 Annual report

Chart

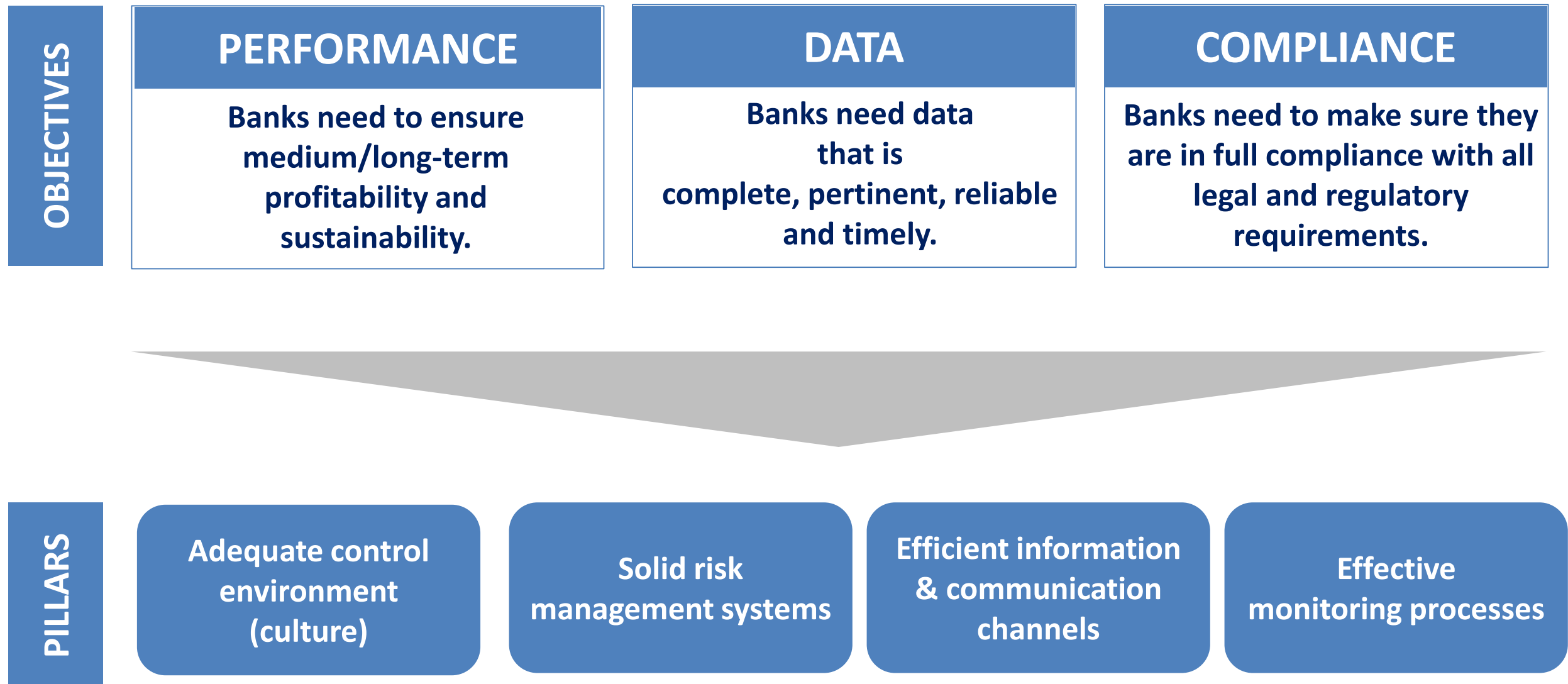
➤ **GRAPHIQUE N° 14 : PERTES LIÉES AU RISQUE OPÉRATIONNEL – RÉPARTITION PAR TYPE D'ÉVÉNEMENT (MOYENNE 2016 À 2024)**



Source: BNP Paribas 2024 Annual report

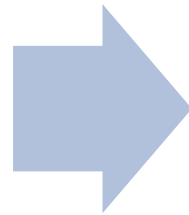
Internal Control

Objectives & pillars



**Internal
Control**

*General framework on
how to approach risks*



**Risk
framework**

*How to control risks
inherent to the bank's
activities in practical
terms*

Risk Appetite Framework

General overview

Risk Appetite Framework

- Banks should identify types of risk the they want to take on and those they wish to avoid.
- Function of: i) appetite to take either a high or a low level of risk on board
ii) capacity of the organisation to take the risk.
- Risk appetite/tolerance levels, thresholds and limits set for the identified material risks must be defined and monitored

Governance framework

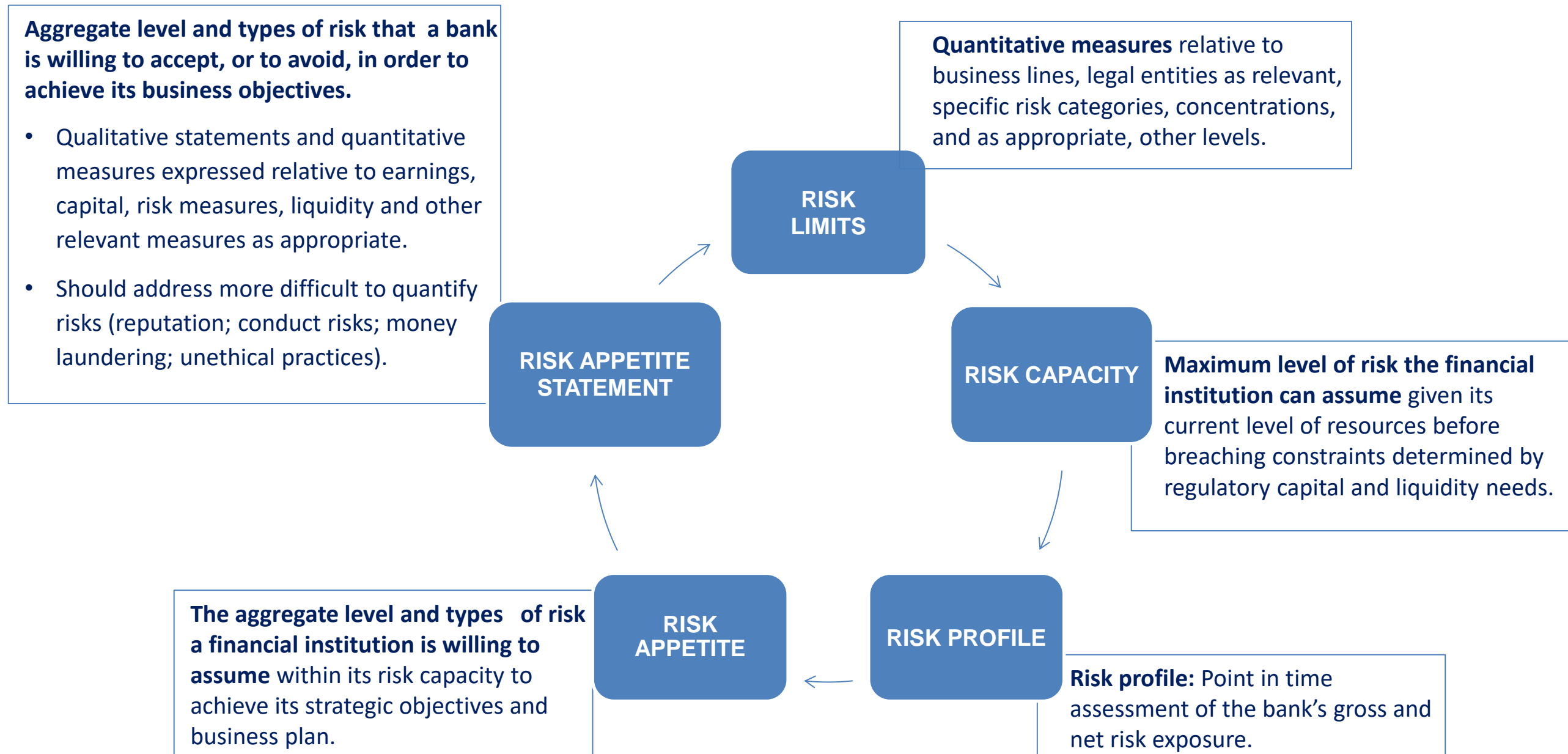
- Banks shall provide information regarding overall governance framework and integration with risk appetite
- The governance structure must ensure integrity of overall business and risk management process.

**Policies, processes, controls
and systems through which
risk appetite is defined, communicated,
and monitored.**

**Material and
reputational risks**

**Alignment
with strategy**

Risk Appetite Framework Components



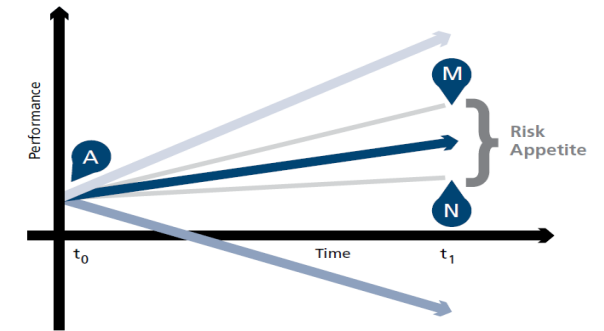
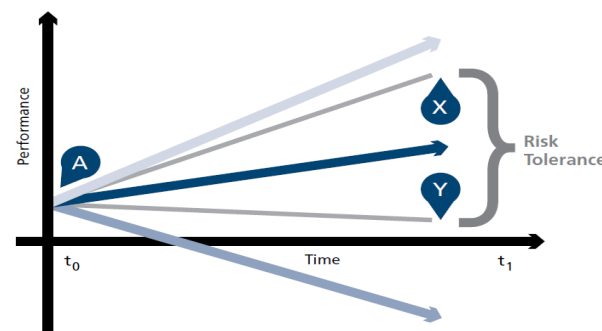
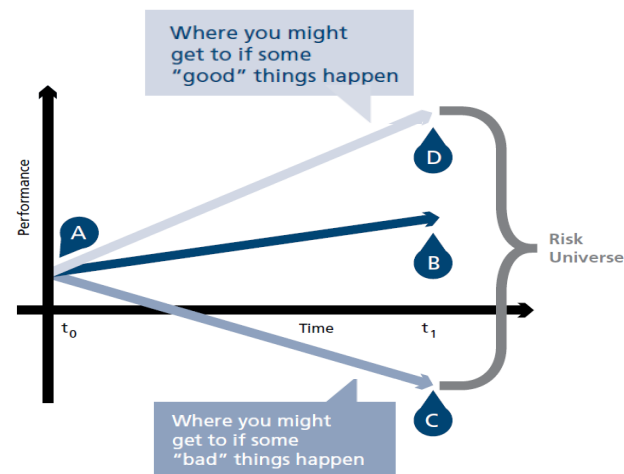
Risk Appetite Framework Applied to Operational Risk

Key point

- When approaching the risks it faces, a bank has four options available in order to control each risk:

- Eliminate
- Mitigate
- Transfer
- Accept

*From risk
tolerance
to risk
appetite*



IMPACT

High	Event can cause substantial damaging impact to strategy/business
Medium	Event can cause visible effects but with limited impact on strategy
Low	Event may be burdensome but has no structural impact



PROBABILITY

High	Highly likely (eg: several times on every quarter)
Medium	May occur at some point in the course of the year
Low	Unlikely, very exceptional



CONTROL'S EFFECTIVENESS

Strong	Control is sufficient to nearly eliminate the risk (>90%)
Acceptable	Mitigation is acceptable (risk reduced to 80-90%)
Low	Mitigation is uncomplete (<80%)
Null	No control has been implemented

Cybersecurity Practice

Creating a technology risk and cyber risk appetite framework

Here's how to build a comprehensive, measurable, and objective end-to-end risk appetite framework as a foundation for managing technology risk and cyber risk.

Case in point

The following is a scenario for the appetite statements and thresholds of each component in a bank's threshold framework. It uses data leakage as an example.

This is an enterprise appetite statement for data leakage risk:

The organization does not tolerate any loss of more than X megabytes of high-sensitivity data a year. It does not tolerate any loss of nonsensitive data that leads to significant reputational damage or to regulatory fines and reviews.

This cascades down to control objectives:

- All vulnerabilities on critical systems must be patched within Y hours of patch release.
- All vulnerabilities on noncritical systems must be patched within Z hours of patch release.
- For the percentage of severity-one, -two, and -three security incidents of data leakage identified through data loss prevention, the metric threshold is B .

The enterprise appetite statement now cascades down to a statement for the business units, such as a retail bank:

The retail bank does not tolerate any loss of more than Y megabytes of high-sensitivity data a year. For nonsensitive data, the retail bank does not tolerate any loss of data that leads to significant reputational damage or regulatory fines and reviews.

Then the organization determines key control indicators and key risk indicators to track enterprise data leakage:

- For the percentage of applications processing critical data with open vulnerabilities, the metric threshold is A percent.

Operational Risk

Possible routes

Business Unit	Business Line	Risk	Event	EI
Retail Bank	Deposits	People	Software failure	Fees
Investment Banking	Cards	Systems	Hardware failure	Fees
Brokerage	Insurance	Processes	Communication Failure	Provisions
		External Events		

Operational Risk Dashboard: an example (I)

■ Compliant ■ Tolerable ■ Unacceptable

Exposure by Risk type	Amber	Red	2018 YTD	Mar	Apr	May	2019 YTD
1 Threshold of 500k€ per event (monthly)	-	≥500k€	1,35M€ 2 incidents	16k€	11k€	71k€	0€ 0 incidents
2 Net Loss Limit ⁽¹⁾ : 3,15M€ (YTD) (265k€ monthly)	≥1,47M€	≥3,15M€	5,3M€	544k€	604k€	798k€	798k€
	≥125k€	≥265k€	-	102k€	57k€	194k€	-
3 Net losses for Operative Risk ⁽¹⁾ : 1,47M€ (YTD)	≥945k€	≥1,47M€	2,8M€	223k€	229k€	334k€	334k€
4 Net losses for External Fraud Risk ⁽¹⁾ : 735k€ (YTD)	≥420k€	≥735k€	879k€	316k€	368k€	433k€	433k€
5 Net losses for Conduct Risk ⁽¹⁾ : 0,5M€ (YTD)	≥120k€	≥0,5M€	1,6M€	15€	2k€	6k€	6k€
6 Net losses for ICT Risk ⁽¹⁾ : 42k€ (YTD)	≥26k€	≥42k€	19k€	4k€	4k€	24k€	24k€
7 Minimum level ≥ 95% incidents (YTD): incidents with insignificant net unit losses (<5k €)	-	<95% incidents	96%	97%	97%	96%	96%
8 Maximum level < 1% incidents (YTD): incidents with material financial impacts (≥100k€)	-	≥1 % incidents	0,9%	0,7%	0,5%	0,4%	0,4%

Operational Risk Dashboard: an example(II)

Operative and IT Risk

■ Compliant ■ Tolerable ■ Unacceptable ■ Not applicable

Type of Risk	Amber	Red	2018 YTD	Mar	Apr	May	2019 YTD
Operative Risk							
Human Resources Risk (scope GNB)							
15 Departure of Employees	≥ 7%	≥ 10%	-	0,2%	0,8%	0,3%	-
16 Absenteeism (YoY)	≥ 3,5%	≥ 5,5%	-	4%	4%	4%	-
17 Exit of High Performance Employees (by their own initiative)	≥ 50%	≥ 66,6%	14 in 105	20%	11%	9%	5 in 42
18 Employees Turnover - Excess Rotation	≥ 3,5%	≥ 5,5%	-	2,2%	4,2%	1,5%	-
Fraud Risk							
21 External Frauds with Cards – Annual budget (YTD) - scope NB	≥ 600k€	≥ 720k€	653k€	99k€	144k€	174k€	-
22 External Frauds with Cards (monthly) - scope NB	≥ 50k€	≥ 60k€	-	53k€	45k€	30k€	-
23 Internal Frauds (monthly) - scope GNB	-	≥ 1 fraud	6	1	0	2	5
24 Internal Frauds (YoY) - scope GNB	> 2 frauds	> 3 frauds	-	8	8	10	-
IT Risk							
Security and Cyber Risk							
30 Unauthorized External Access	-	≥ 1 incident	0	0	0	0	0
31 Systems data loss (malware)	-	≥ 1 system	0	0	0	0	0
32 PC data loss (malware)	≥ 1PC	≥ 2PC	0	0	0	0	0
33 Home banking Attacks (impacted clients)	≥ 1 Client	≥ 5 Clients	1	0	0	0	0
Continuity Risk							
34 High Severity Systems Incidents	≥1 incident	≥ 3 incidents	5	0	0	0	2
35 Systems Downtime >8h	≥1 incident >8h	≥ 3 incidents >8h	2	0	0	0	1

Operational Risk

Dashboard: an example (III)

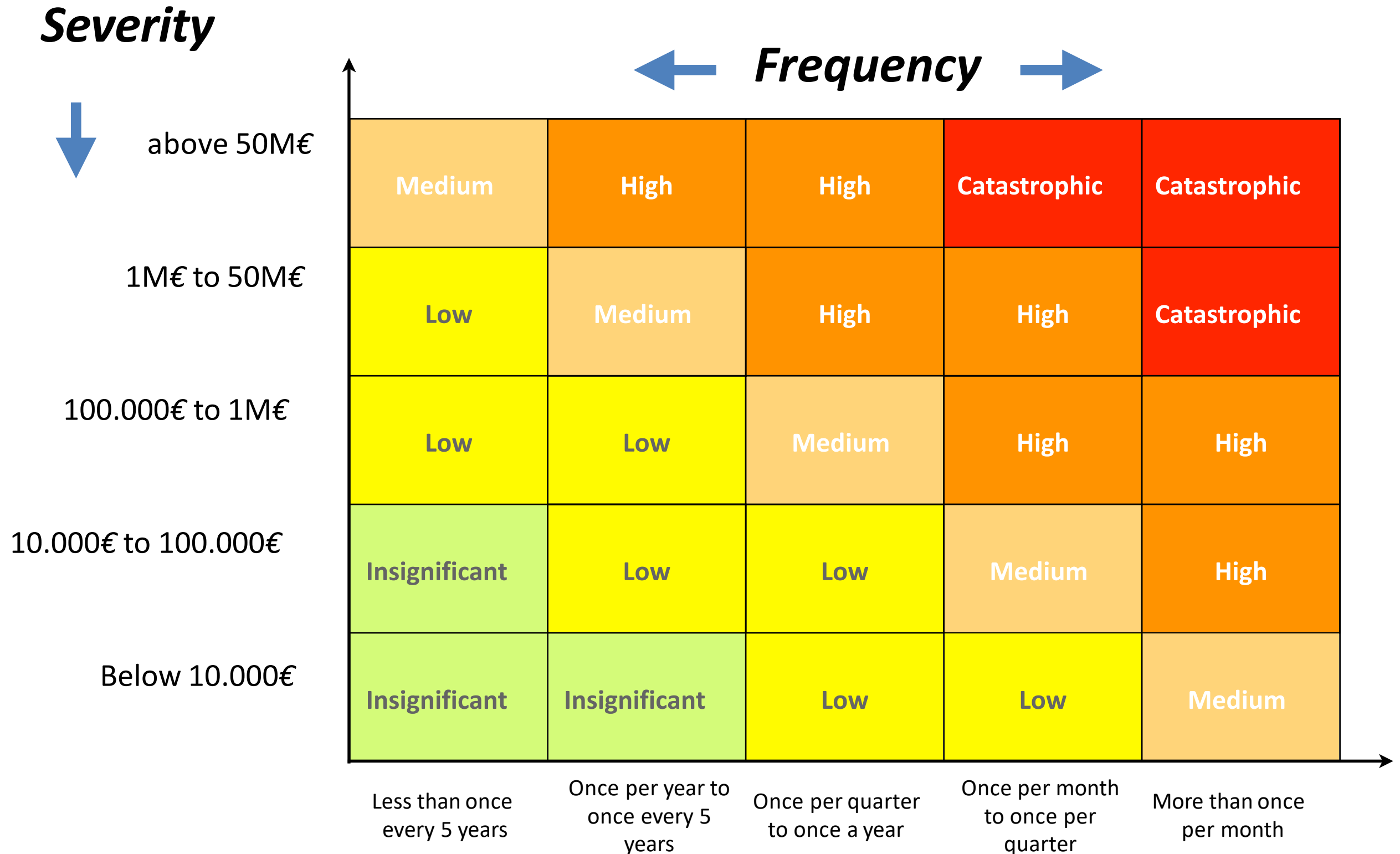
Compliance Risk Appetite (1/3)

■ Compliant ■ Tolerable ■ Unacceptable ■ Not applicable

Compliance Risk Appetite	Amber	Red	2018 YTD	Mar	Apr	May	2019 YTD
Compliance with laws & regulations (scope GNB)							
37 Regulatory fines	-	≥ 1 fine	10	0	0	0	0
38 Other Entity fines Unit Values	≥ 2k€	≥ 4k€	4	0	0	0	1
39 Delay in sending Regulatory Reports (working days)	-	≥ 1 day	178	3	19	2	41
Transparency degree (scope NB)							
40 Specific determinations (1)	-	≥ 5 incidents	8	0	1	1	2
Involvement in money laundering operations (scope NB) (2)							
41 AML- Requests to terminate contracts (SLA 10 calendar days)	-	≥ 1 contract	4	0	0	0	0
42 FT- Requests to terminate contract (SLA 10 calendar days)			0	0	0	0	0
43 AML - Requests to finalize the business relationship (SLA 90 calendar days)			14	0	0	0	18
44 FT- Requests to finalize the business relationship (SLA 90 calendar days)			0	0	0	0	0
Responsibilities to 3 rd parties (scope NB)							
45 Legal action against NB under the resolution measure (YTD)	≥ 10	≥ 48	48	4	5	5	-
46 Legal actions against NB within core banking activity (YTD)	≥ 8	≥ 42	42	19	31	34	-

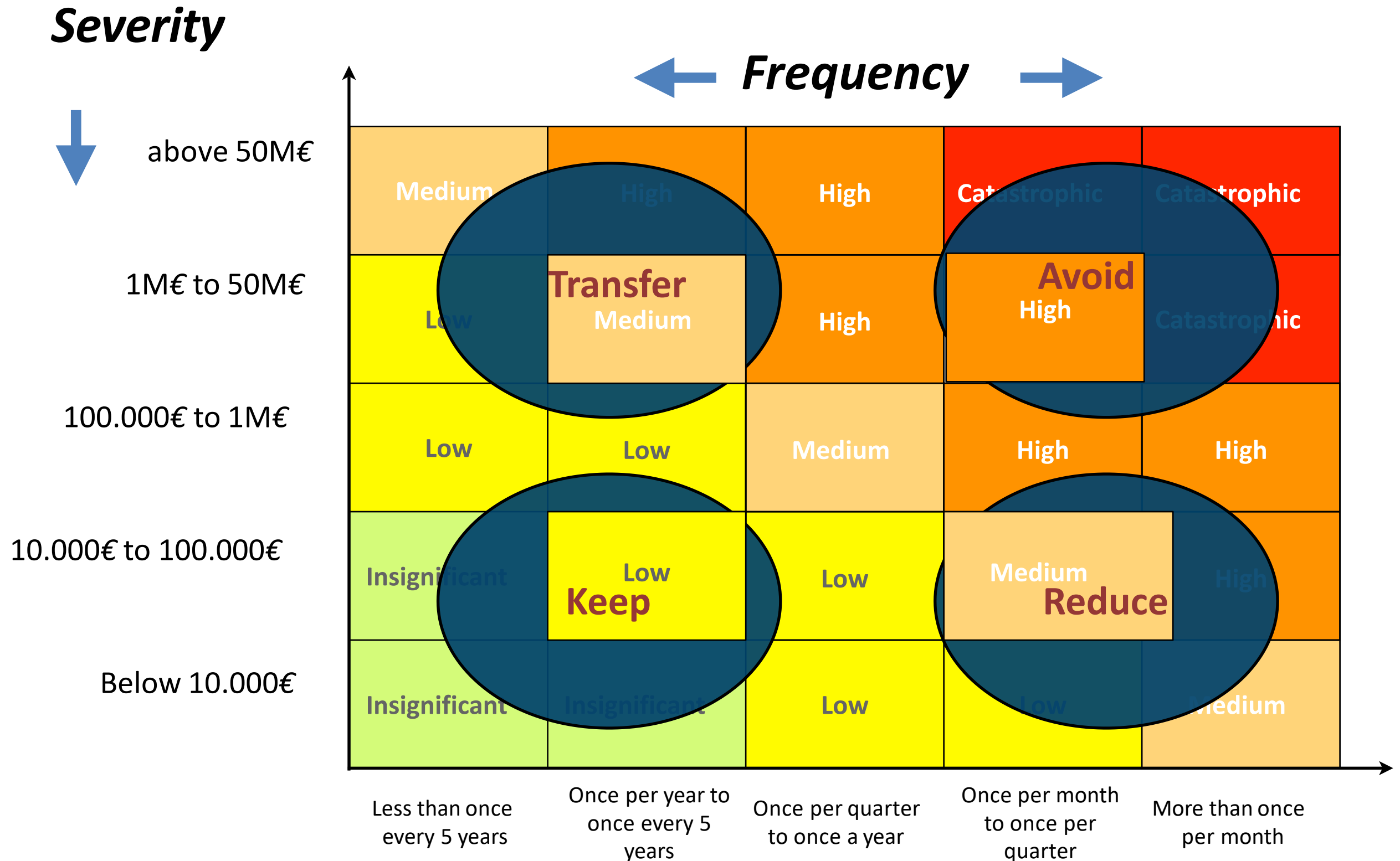
Risk Tolerance Matrix

How it works



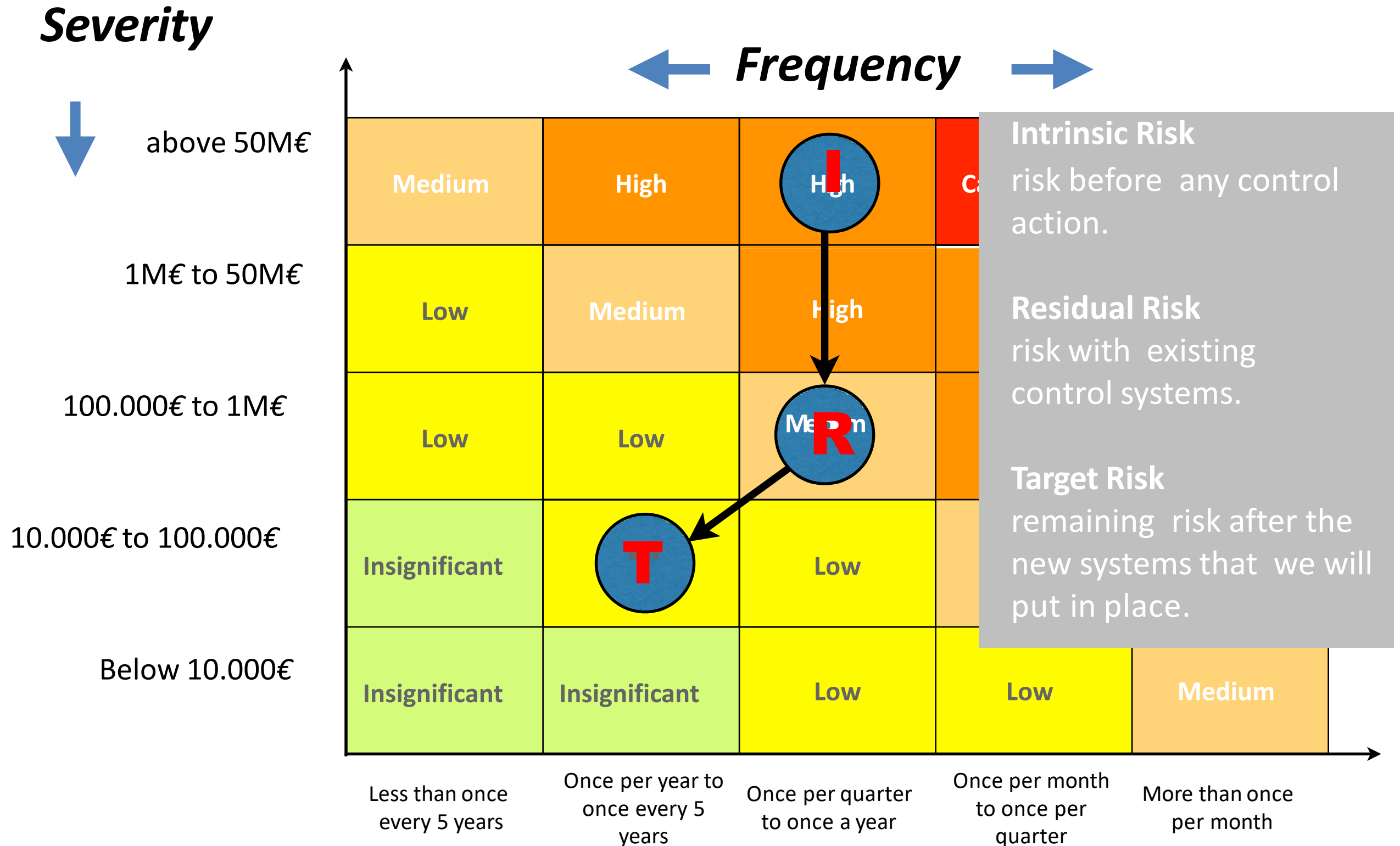
Risk Tolerance Matrix

Possible strategies



Risk Tolerance Matrix

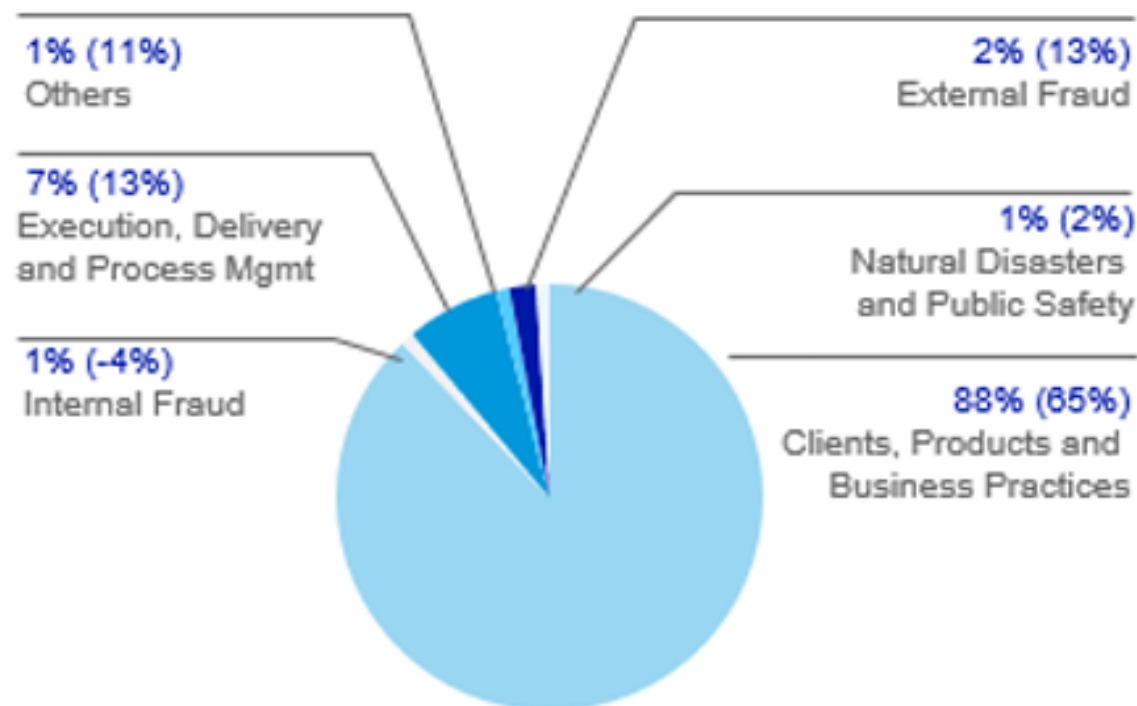
Outcomes



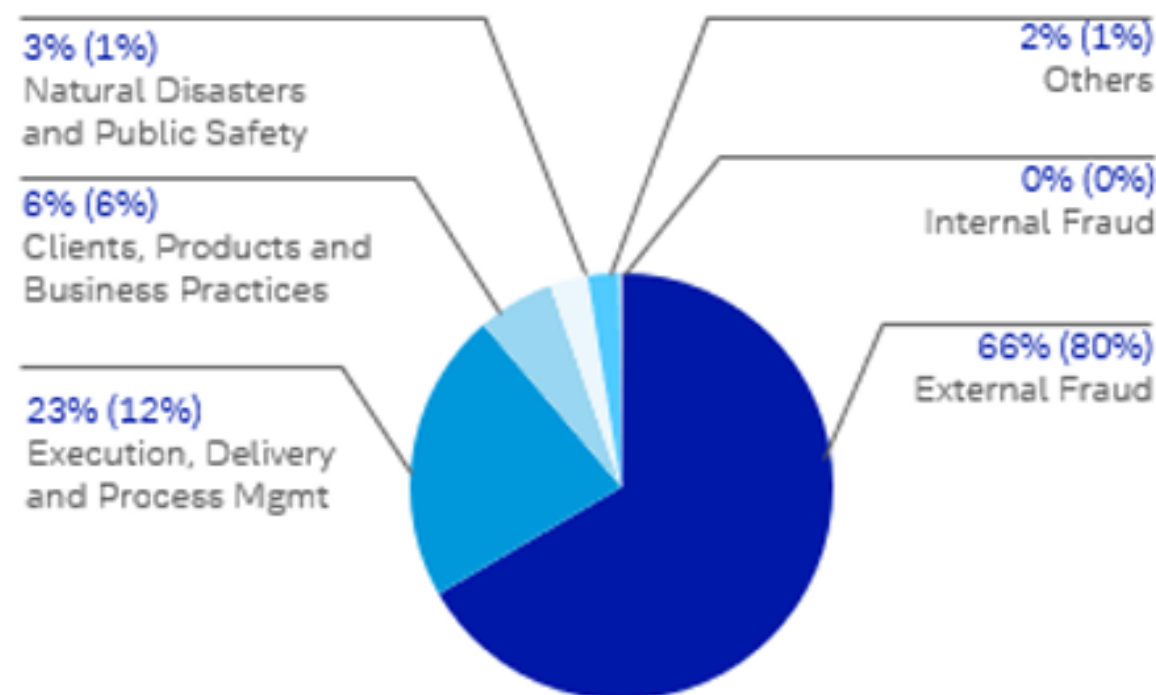
Operational Risk

Main categories

Distribution of Operational Losses²



Frequency of Operational Losses³



¹ Prior year losses have been revised to account for subsequent capture of losses and reclassification

² Distribution of operational risk losses is based on posting date

³ Frequency of operational risk losses is based on first posting date

⁴ The bank seeks to ensure the comprehensive capture of all operational risk loss events with a net operational risk loss impact of € 10,000 or greater, the totals shown in this section may be underestimated due to delayed detection and recording of loss events

**Key
concept**

Banks are required to “have adequate policies and processes (...) to prevent the bank from being used, intentionally or unintentionally, for criminal activities”.

A bank must develop a thorough understanding of the inherent ML/FT risks present in its customer base, products, delivery channels and services offered and jurisdictions within which it or its customers do business.

CDD: Customer Due Diligence

KYC: KNOW YOUR CUSTOMER

- Onboarding: banks must have clear customer acceptance policies and procedures to identify the types of customer that are likely to pose a higher risk of ML/FT.
- A bank should not establish a banking relationship or carry out any transactions until the identity of the customer has been satisfactorily established and verified.



PEP: Politically Exposed Person
UBO: Ultimate Beneficiary Owner






KYT: KNOW YOUR TRANSACTION

- A bank should have a transaction monitoring system in place that allows it to collect sufficient specific operational and transaction data as well as other internal information.

Operational risk in AML/CTF






An example: KYC monitoring rules

Onboarding and periodic diligences and procedures should be carried out to ensure the timeliness, accuracy and completeness of the clients' information

#	 Alert	 Description	 Objective	 Frequency	 Owner
1	Filtering: Sanctions, PEP and blacklists	Filtering all entities (clients, UBO's, legal representatives, proxies) during the onboarding phase and at the client review phase. In case of a match with a list, an alert should be generated.	Check the presence of: i) Sanctioned entities (compliance with article 21.º of Law n.º 83/2017); ii) PEP (compliance with article 39.º of Law n.º 83/2017); iii) undesirable clients.	1. Whenever it occurs; 2. Real Time.	Compliance Department
2	Onboarding: high risk clients	Alert when a high risk entity is trying to onboard.	Immediate aware of high risk clients onboarding the bank, in order to perform the necessary diligences.	1. Whenever it occurs; 2. Real Time.	Compliance Department
3	Onboarding: PEP entities (manual)	Alert when there is the identification of a PEP entity during the onboarding that is not present in the external lists.	Compliance with article 39.º of Law n.º 83/2017) to identify all PEP clients and manually mark them in the system.	1. Whenever it occurs; 2. Real Time.	Compliance Department
4	Clients' with high risk activity sectors	Alert when an client with a high risk activity sector is trying to onboard.	Immediate aware of clients connected to high risk activity sectors onboarding the bank, to perform additional diligences.	1. Whenever it occurs; 2. Real Time.	Commercial & Compliance Departments

Operational risk in AML/CTF

An example: KYT monitoring rules

#	 Alert	 Description	 Objective	 Frequency	 Owner
4	Smurfing - Cash deposits by a third party*	<p>For low and medium risk clients, several cash deposits that together account for:</p> <ul style="list-style-type: none"> i) € 10 000 in 7 days; ii) € 25 000 in 30 days. <hr/> <p>For high risk clients, several cash deposits that together account for:</p> <ul style="list-style-type: none"> i) € 5 000 in 7 days; ii) € 15 000 in 30 days. 	Detect the fractioning of cash deposits in order to disguise the origins of the funds.	Batch – Weekly	Compliance Department
5	Large cash withdrawal*	Cash withdrawal of an amount equal or greater than € 10 000.	Determine the destination of the funds being withdrawn.	Batch– Daily	Compliance Department
6	Account open followed by withdrawal	Detect recently opened accounts where within 5 days 90% of the initial amount is withdrawn or transferred.	Understand the reasoning for the opening of the account and the destination of the funds.	Batch – Daily	Compliance Department
7	Quick in and out	Funds entering the clients' account over € 15 000 and 90% of the amounts is quickly transferred or withdrawn from the account within two days.	Detect possible layering of funds.	Batch – Daily	Compliance Department

Operational risk in AML/CTF

Danske Bank: when things go wrong

Danske: anatomy of a money laundering scandal

How the Danish bank found itself at the centre of a €200bn money laundering scandal



© FT montage / Getty / Bloomberg

Richard Milne and Daniel Winter DECEMBER 19, 2018

11

<https://next-media-api.ft.com/renditions/15408984157690/1280x720.mp4>

Danske Bank warns profits could almost halve this year

Money-laundering scandal and negative rates weigh on biggest Danish lender



Source: FT, 5 Feb 2020

All charges dropped against Danske Bank chiefs

Denmark's state prosecutor concludes that no gross negligence was committed by individuals in €200bn scandal



Source: FT, 29 Apr 2021

Danske Bank to pay \$2bn penalty for defrauding US banks

Denmark's largest lender pleads guilty to resolve one of the biggest money-laundering scandals in years

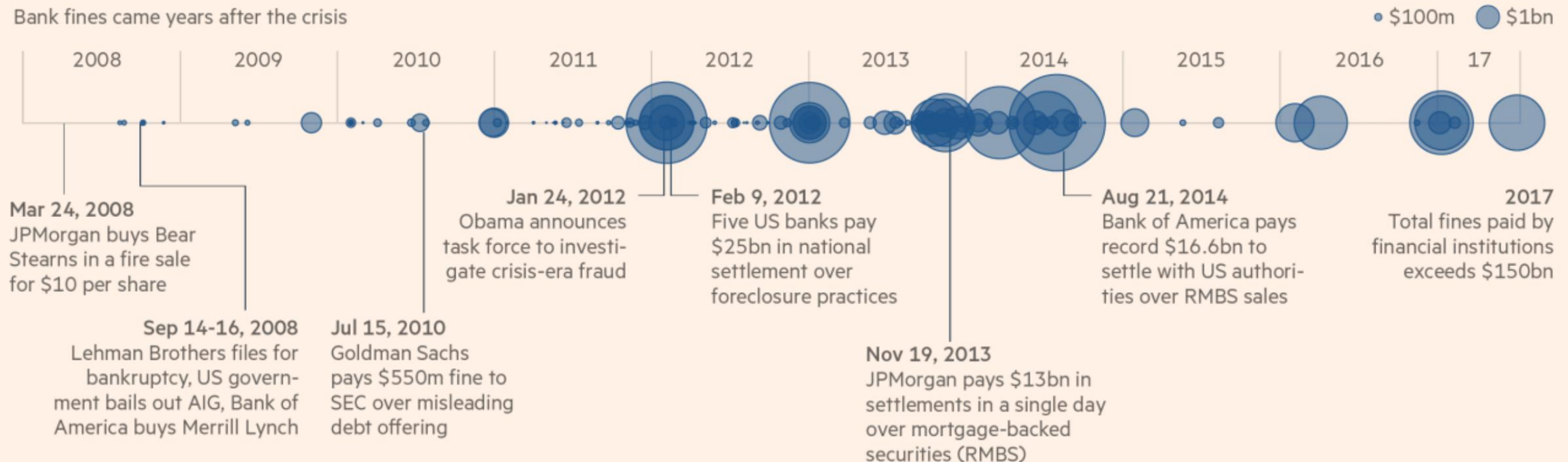


Source: FT, 13 Dec 2022

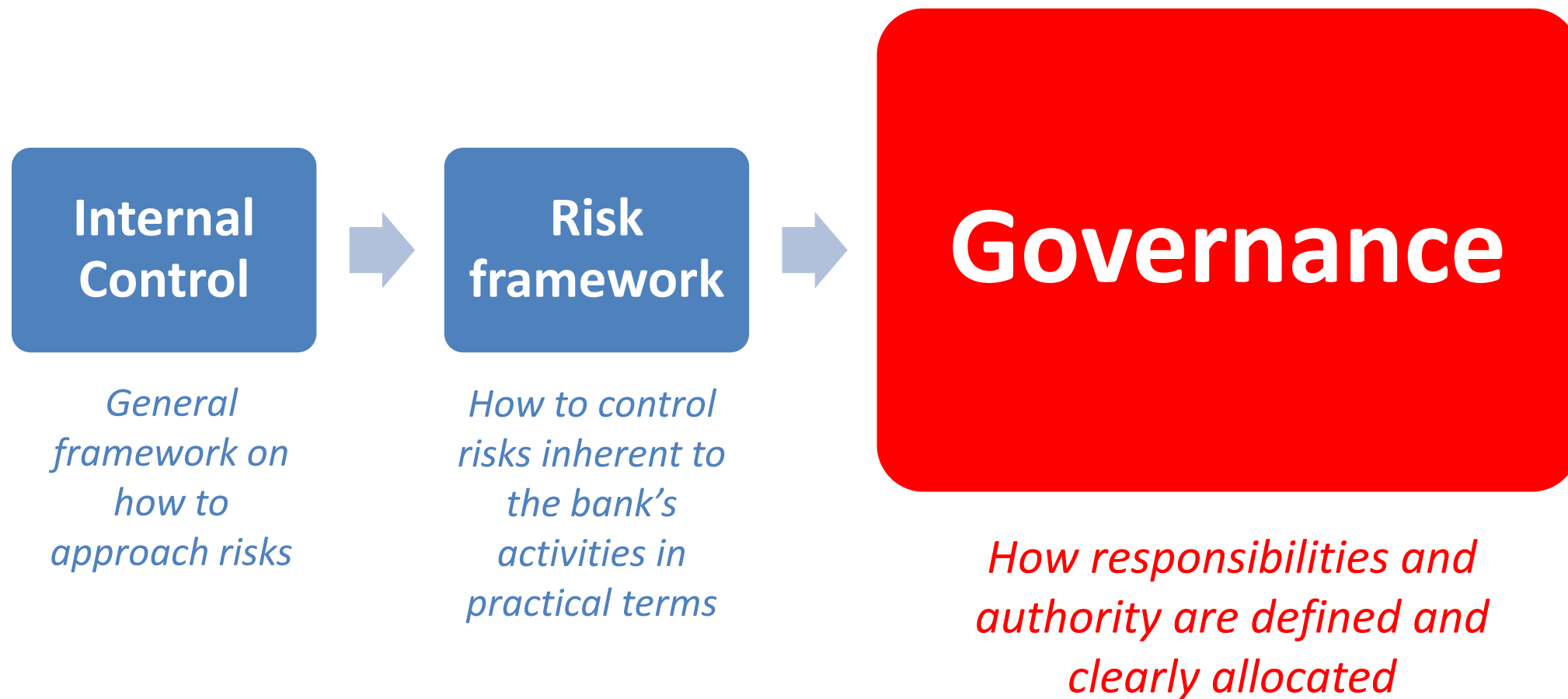
FEBRUARY 21, 2019		European banks SEC joins list of authorities probing Danske money laundering Swedbank appoints EY to investigate potential link in €200bn scandal	Save
FEBRUARY 20, 2019		European banks Swedbank shares plummet on link to Danske scandal Swedish broadcaster alleges bank handled \$5.8bn of suspicious fund flows to Danish rival	Save
FEBRUARY 19, 2019		Estonian scandal forces Danske out of the Baltics and Russia EU's banking regulator launches probe into Danish and Estonian watchdogs	Save
FEBRUARY 15, 2019		Deutsche Bank AG Germany deepens probe into Deutsche's role in Danske arm Financial watchdog widens remit of independent auditor at largest German lender	Save
FEBRUARY 4, 2019		Danske faces new front in money-laundering scandal Leading shareholder adviser files motion for AGM calling for independent probe	Save

MENTI TIME 😊

The long road



Graphic by Claire Manibog, Kara Scannell and Cleve Jones Source: FT research
© FT



Risk Management

The 3-line of defence approach

1ST LINE: FRONT-OFFICE

- Business units (front office, customer-facing activity) are the first responsible for identifying, assessing and controlling the risks of business.
- Internal policies and procedures should be clearly specified in writing and communicated to all personnel.

2ND LINE

Risk officer

- Facilitates implementation of risk management framework;
- Responsible for further identifying, monitoring, analysing, measuring, managing and reporting on risks (holistic view on all risks);
- Challenges and assists in implementation of risk management measures by the business lines

=> ensure process and controls at the first line of defence are properly designed and effective.

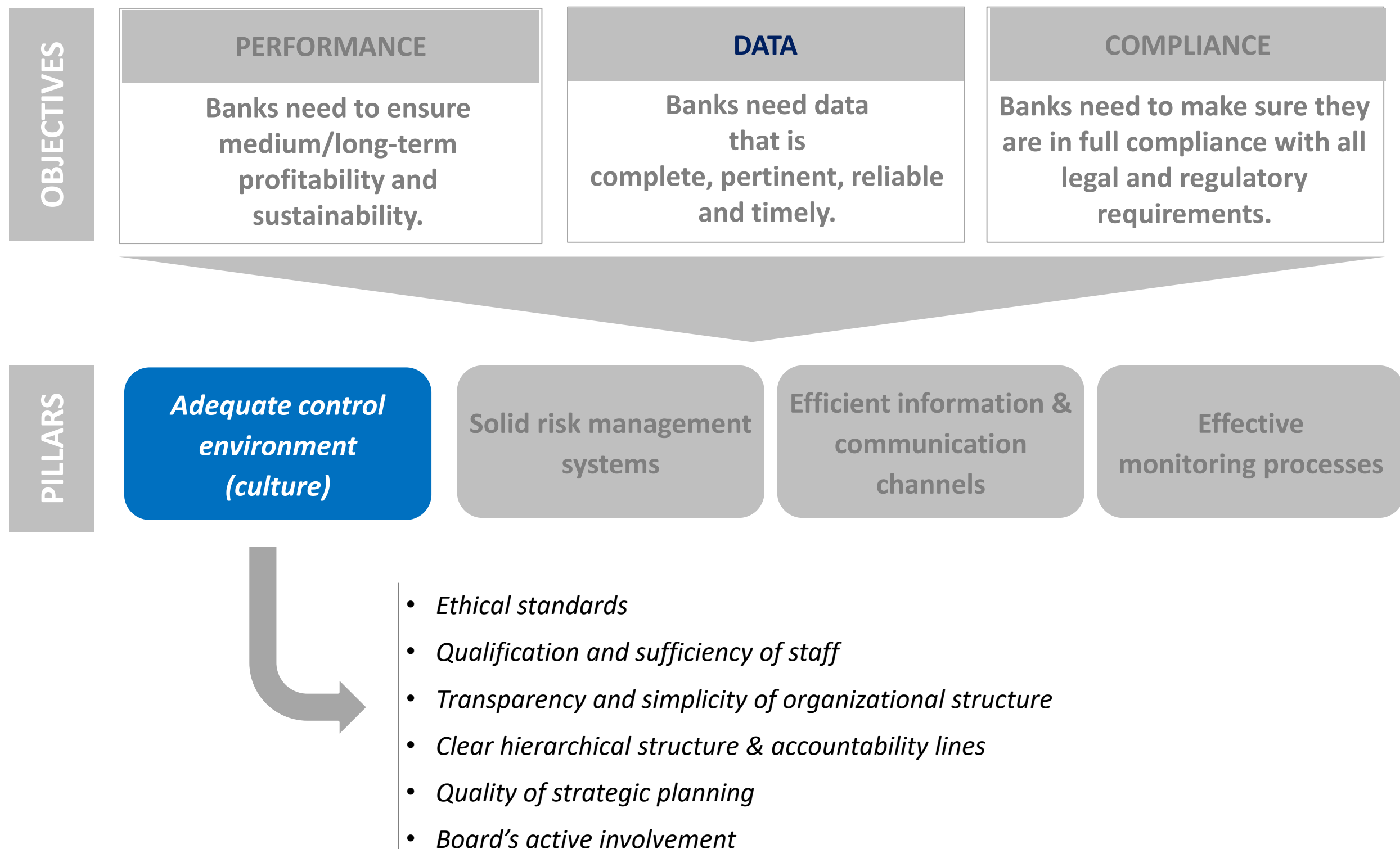
Compliance officer

- Monitors compliance with legal and regulatory requirements and internal policies
- Provides advice on compliance to the management body and other relevant staff,
- Establishes policies and processes to manage compliance risks and to ensure compliance.

3RD LINE: INTERNAL AUDIT

- Conducts risk-based and general audits;
- Reviews internal governance arrangements, processes and mechanisms to ascertain that they are sound and effective, implemented and consistently applied.
- Carries independent review of the first two lines of defence.

All internal control functions need to be independent of the business they control, have the appropriate financial and human resources to perform their tasks, and report directly to the management body.



INTERNAL GOVERNANCE

...tackles...

- Standards and principles concerned with setting an institution's objectives, strategies and risk management framework;
- how business is organised;
- how responsibilities and authority are defined and clearly allocated;
- how reporting lines are set up and what information they convey;
- how the internal control framework is organised and implemented, including accounting procedures and remuneration policies
- how sound information technology systems are
- the nature of outsourcing arrangements
- business continuity management.

*...subject to Principle
of proportionality*

Requirements are to be applied in a manner that is appropriate, taking into account in particular the institution's size, internal organisation and nature, and the complexity of its activities.

Management body:

- Business strategy
- Risk strategy
- Internal control

Management function (executive members)

- Active involvement in day-to-day business; decisions should be taken on a sound and well-informed basis

Supervisory function (non-executive members)

- Monitor and constructively challenge strategy
- Monitor risk culture and governance's effectiveness

"The chair should encourage and promote open and critical discussion and ensure that dissenting views can be expressed and discussed within the decision-making process."

Committees

Risk

- Supports Supervisory body in its assessment of risk appetite framework

Audit

- Monitors the effectiveness of internal quality control and risk management systems

Others

- Nomination, Remuneration

Must be chaired by independent / non-executive directors

Internal Control functions

Risk

- Risk day-to-day management

Compliance

- Ensures bank is fully compliant with all required legislation and regulation across the entire organization

Audit

- Assesses adequacy of governance, policies and robustness of controls/ procedures

- *Must be independent from activities they are supposed to control*
- *Remuneration cannot be linked to performance*

Context

“Weaknesses in corporate governance, including inadequate oversight by and challenge from the supervisory function of the management body in a number of credit institutions and investment firms, have contributed to excessive and imprudent risk-taking in the financial sector which has led in turn to the failure of individual institutions and systemic problems.” (EBA)

Requirements for members of management body

- Sufficient time to carry out their respective responsibilities appropriately.
- Sufficient time to acquire, maintain and enhance their knowledge and skills – if necessary through additional training.
- Must be of good repute.
- Should be able to demonstrate independence of mind to be able to effectively assess, challenge, oversee and monitor management decision-making.

Final regulator's approval on the composition of a management board will depend on the collective assessment of the combination of competencies and skills of all members

Collective
assessment
template

This is the non-exhaustive list of relevant skills, referred to in paragraph 61, that institutions should consider using when performing their suitability assessments:

- a. **Authenticity:** is consistent in word and deed and behaves in accordance with own stated values and beliefs. Openly communicates his or her intentions, ideas and feelings, encourages an environment of openness and honesty, and correctly informs the supervisor about the actual situation, at the same time acknowledging risks and problems.
- b. **Language:** is able to communicate orally in a structured and conventional way and write in the national language or the working language of the institution's location.
- c. **Decisiveness:** takes timely and well-informed decisions by acting promptly or by committing to a particular course of action, for example by expressing his or her views and not procrastinating.
- d. **Communication:** is capable of conveying a message in an understandable and acceptable manner, and in an appropriate form. Focuses on providing and obtaining clarity and transparency and encourages active feedback.
- e. **Judgement:** is capable of weighing up data and different courses of action and coming to a logical conclusion. Examines, recognises and understands the essential elements and issues. Has the breadth of vision to look beyond his or her own area of responsibility, especially when dealing with problems that may jeopardise the continuity of the undertaking.
- f. **Customer and quality-oriented:** focuses on providing quality and, wherever possible, finding ways of improving this. Specifically, this means withholding consent from the development and marketing of products and services and to capital expenditure, e.g. on products, office buildings or holdings, in circumstances where he or she is unable to gauge the risks properly owing to a lack of understanding of the architecture, principles or basic assumptions. Identifies and studies the wishes and needs of customers, ensures that customers run no unnecessary risks and arranges for the provision of correct, complete and balanced information to customers.
- g. **Leadership:** provides direction and guidance to a group, develops and maintains teamwork, motivates and encourages the available human resources and ensures that members of staff have the professional competence to achieve a particular goal. Is receptive to criticism and provides scope for critical debate.
- h. **Loyalty:** identifies with the undertaking and has a sense of involvement. Shows that he or she can devote sufficient time to the job and can discharge his or her duties properly, defends the interests of the undertaking and operates objectively and critically. Recognises and anticipates potential conflicts of personal and business interest.
- i. **External awareness:** monitors developments, power bases and attitudes within the undertaking. Is well-informed on relevant financial, economic, social and other developments at national and international level that may affect the undertaking and also on the interests of stakeholders and is able to put this information to effective use.
- j. **Negotiating:** identifies and reveals common interests in a manner designed to build consensus, while pursuing the negotiation objectives.
- k. **Persuasive:** is capable of influencing the views of others by exercising persuasive powers and using natural authority and tact. Is a strong personality and capable of standing firm.
- l. **Teamwork:** is aware of the group interest and makes a contribution to the common result; able to function as part of a team.
- m. **Strategic acumen:** is capable of developing a realistic vision of future developments and translating this into long-term objectives, for example by applying scenario analysis. In doing so, takes proper account of risks that the undertaking is exposed to and takes appropriate measures to control them.
- n. **Stress resistance:** is resilient and able to perform consistently even when under great pressure and in times of uncertainty.
- o. **Sense of responsibility:** understands internal and external interests, evaluates them carefully and renders account for them. Has the capacity to learn and realises that his or her actions affect the interests of stakeholders.
- p. **Chairing meetings:** is capable of chairing meetings efficiently and effectively and creating an open atmosphere that encourages everyone to participate on an equal footing; is aware of other people's duties and responsibilities.

Context

“Inappropriate remuneration structures have been a contributing factor to excessive and imprudent risk taking. Poorly designed remuneration policies have potentially detrimental effects on the sound management of risks, control of risk and the risk-taking behaviour of individuals”.
(EBA)

“Remuneration has a direct or indirect influence on staff’s behaviour. Variable remuneration may encourage staff to take undesirable, irresponsible and excessive risks or to sell unsuitable products in the hope of generating more turnover or making more profit in the short run and thus increasing staff’s variable remuneration. Furthermore, staff members may be tempted to game with or manipulate information with a view to making their (measured) performance look better”.

Remuneration Rules

Fixed remuneration

- Permanent, predetermined, non-discretionary and non-revocable.
- Should primarily reflect relevant professional experience and organisational responsibility of staff while providing a stable source of income.

Variable remuneration

- Based on performance or, in exceptional cases, other conditions.
- Should provide incentives for prudent risk taking in the long term and sound risk management.
- **At least 50% of variable remuneration must comprise** a balance of shares, equivalent ownership rights, share-linked or equivalent **non-cash instruments**, in the case of non-listed institutions, and, where possible, certain eligible other instruments defined within.
- **At least 40% of variable remuneration is subject to deferral arrangements.** The awarded instruments are subject to retention periods.

Operational risk

When it's about culture

Goldman Sachs sued over work on \$2.9bn grocery deal

Bank accused of manipulating credit default swaps market and taking excessive fees



© Reuters

Laura Noonan in New York JANUARY 31, 2019

25

Morgan Stanley

+ Add to myFT

Morgan Stanley discloses twin probes into big stock transactions

Wall Street bank says SEC and justice department have sought information on block trades



Source: FT, 24 Feb 2022.

Exam suggestion:

Write a short summary on:

- . the nature of the problem at stake,
- . How could adequate Governance models have avoided the probes

MENTI TIME 😊

Potential €50m bill forces Santander U-turn on Orcel

Spanish lender says it cannot justify amount to install banker from UBS as new chief



Santander said the compensation due to Andrea Orcel would be 'significantly above the board's original expectations' © Bloomberg

David Crow, Banking Editor JANUARY 15, 2019

Spanish court upholds Andrea Orcel's Santander claim but cuts payout by €8mn

Bank ordered to pay €43.5mn in compensation for aborted offer but will appeal to Supreme Court



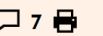
Source: FT, 6 Feb 2023.

Remuneration When it goes wrong

Santander/Orcel: no we cannot

Spanish bank may have dodged a bullet over lost pay from UBS

JANUARY 16, 2019



Is there no end to the havoc caused by rising populism? Chaos in UK politics and in Paris was bad enough. But things have come to a dire pass when a banker cannot switch jobs without losing upwards of €50m in back pay.

[Banco Santander](#) changed its mind about [hiring Andrea Orcel](#) as chief executive partly because Spanish politics changed. Since last year the centre-left Spanish Socialist Workers' Party has ruled with unreliable support from anti-austerity populists Podemos (translation: "yes we can").

Distrust of bankers has been deepening. It would have been sticky for Santander to cover half the income Mr Orcel stood to lose after quitting as head of investment banking at UBS. There was no way the Spanish bank could shell out the full €50m-plus after the Swiss bank declined to pay the other half. UBS had decided it would do no favours to one of its biggest clients.

Another pay drama starring Andrea Orcel

European banking's MVP is up for a pay review

They don't call **Andrea Orcel** the "Ronaldo of Bankers" for nothing.

Much like the Portuguese football star, the banker is known for pulling off big wins and collecting generous payouts in the process.

So two years into his role as chief executive of **UniCredit**, the bank's board is considering raising his €7.5mn salary by 20 to 30 per cent. But DD readers know that it wouldn't be a conversation about Orcel's pay without a little controversy.

After helping boost UniCredit's share price from €11 to €19 in less than two years and helping generate record profits in 2022, Orcel's gains [have been overshadowed](#) by a series of controversies that have raised questions over his leadership style and corporate governance at the Milan-based lender, the FT reports.

Source: FT, 28 Feb 2023.

Capital requirements

Calculation approaches

Basic indicator approach

- Average of last 3 years of the Gross Income x 15%

Standardised approach

- Approach by business lines defined by the regulator
- A single exposure indicator: the Gross Income of each businessline (average of last 3 years)
- A weighting factor α by business line reflects the risk related to the activity
- Qualifying criteria

Advanced measurement approach

- Development of an internal measurement model based on eight business lines and seven risk categories defined by the regulator
- Qualifying criteria

Capital requirement

Sophistication

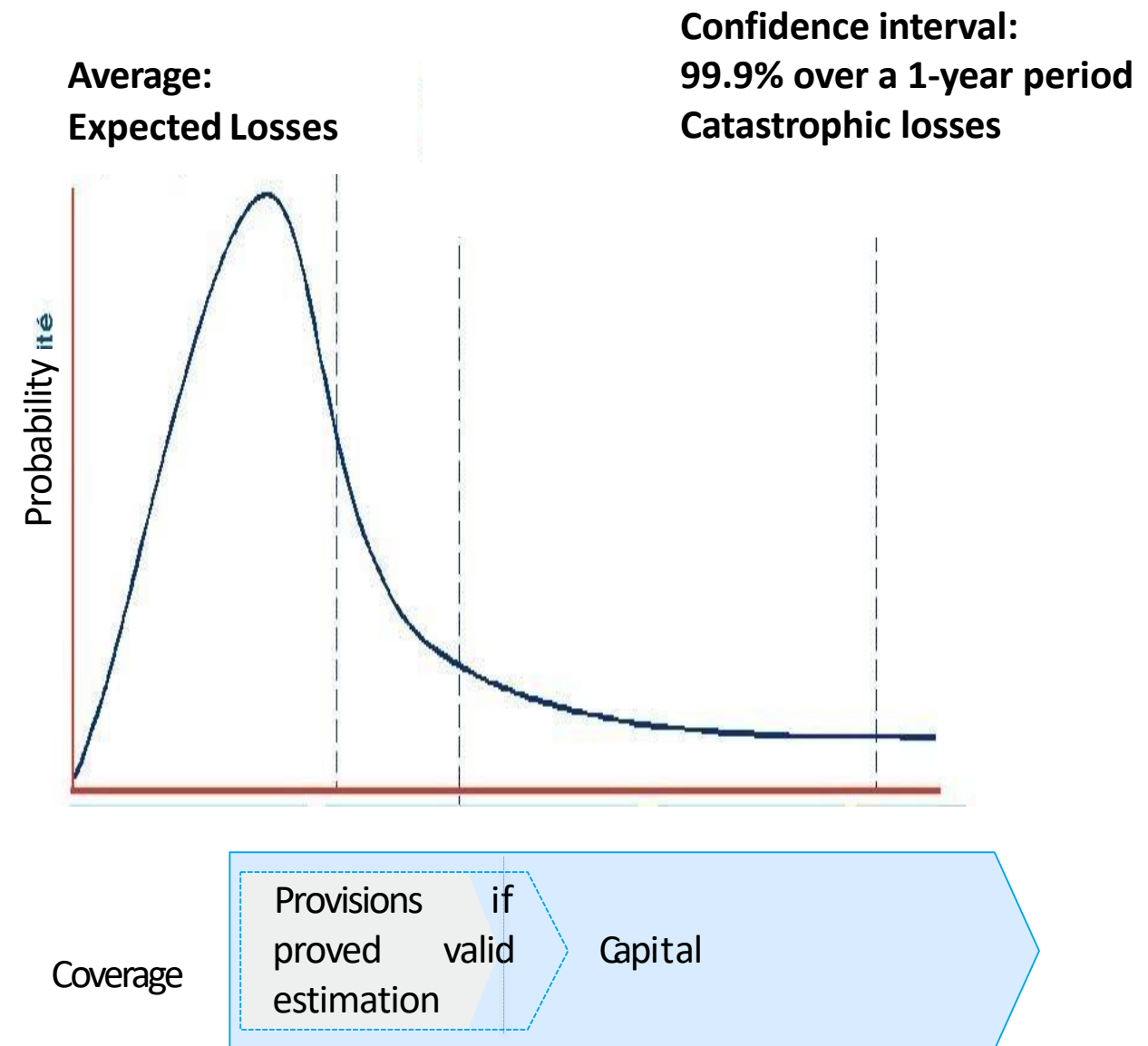
Capital requirements

AMA: the future?

- The capital requirement is calculated using an internal model developed by the bank under qualitative and quantitative constraints:

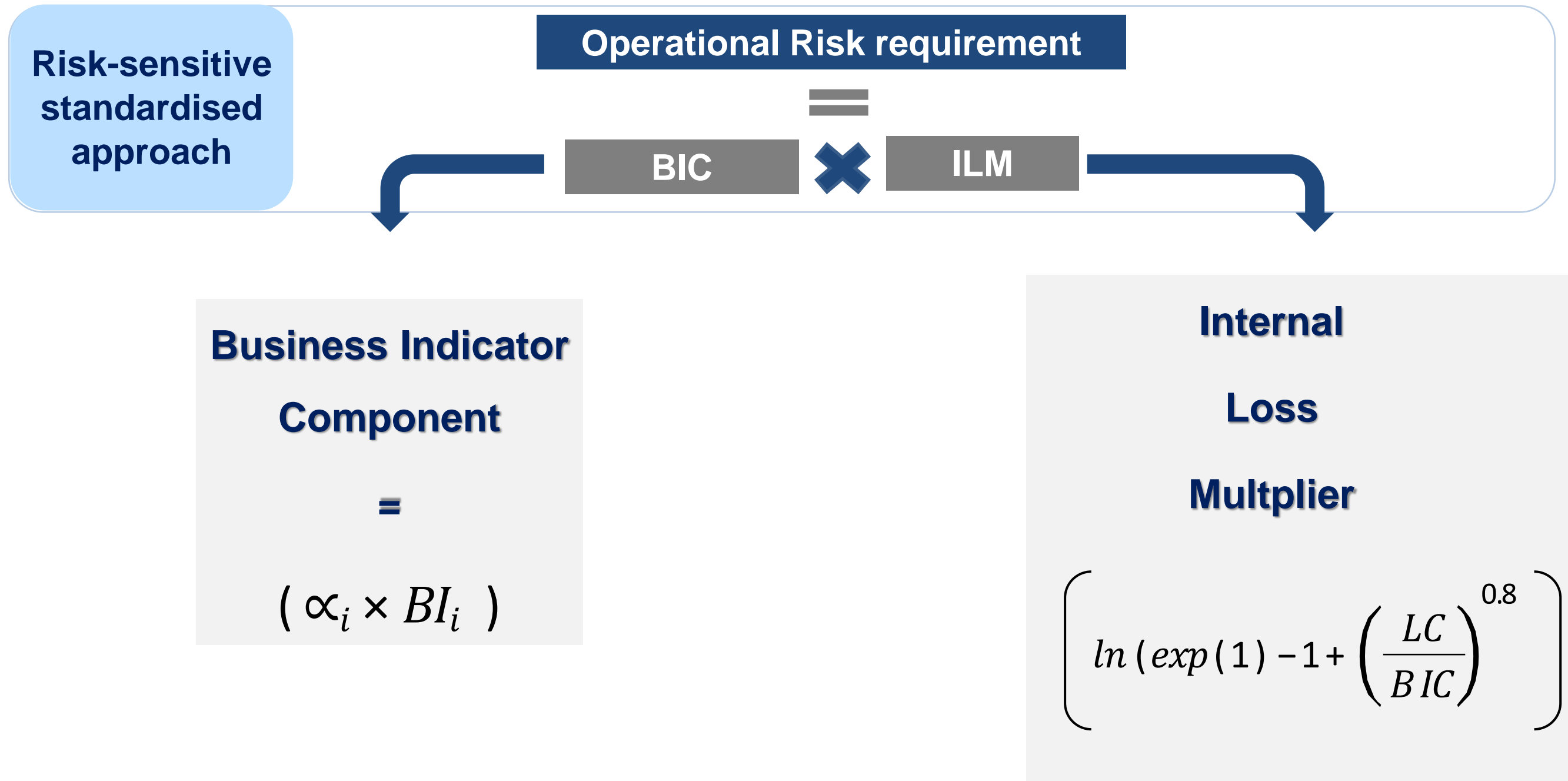
$$K_{AMA} = EL + UL$$

- If the bank demonstrates that it is adequately capturing EL in its internal business practices, the base to capital requirements can be UL alone.
- Few details are given on the calculation methods used by this model.
- The effective use of an internal model is subject to the prior approval by the regulator.



However, AMA has presented some practical problems...

- Difficulty in modelling extreme events is related with the absence of data for rare events.
- Insufficient data on extreme events makes it necessary to consider external data and experts' opinions.



Operational Risk